In the specification:

In the abstract:

Please replace the abstract of the disclosure on page 23 as follows:

Tokenless biometric authorization of ~~an electronic~~ transaction between a consumer and a merchant uses an ~~electronic~~ identicator and an access device. ~~The access device need not contain data personalized to the consumer.~~ A consumer registers with the identicator a ~~registration~~ biometric sample taken from the ~~consumer's person~~ consumer. The consumer and merchant establish ~~mutual~~ communications via the access device. The merchant proposes a ~~commercial~~ transaction to the consumer via the access device. The access device communicates to the merchant ~~an identification code~~ associated with the access device. After the consumer and merchant have agreed on the transaction, the consumer and the identicator use the access device to establish ~~mutual~~ communications. The access device communicates to the identicator the ~~identification~~ code associated with the access device. The identicator compares ~~a bid~~ biometric sample from the consumer with registered biometric sample ~~to try to identify the consumer~~. Upon successful identification, the identicator ~~electronically~~ forwards information regarding the consumer to the merchant. These steps accomplish a biometrically authorized electronic financial transaction without the consumer having to present any personalized man-made memory tokens.

Please replace the first full paragraph on page 1, lines 8-9 with the following paragraph:

This application claims ~~priority from~~ the benefit of U.S. provisional application Serial No. 60/208,680, filed May 31, 2000.

Please replace paragraph 5, starting at line 19 on page 4 and ending at line 14 on page 5 with the following paragraph:

This invention provides a method for tokenless biometric authorization of an electronic transaction between a consumer and a merchant using an electronic identicator and an access device. The method comprises the following steps: In a consumer registration step, a consumer registers with the electronic identicator at least one registration biometric sample taken directly from the consumer's person. In a first communications establishment step, the consumer and merchant establish communications with each other via an access device capable of biometric input, and wherein the access device is not required to contain in memory any data that is personalized to the consumer. In a proposal step, the merchant proposes a commercial transaction to the consumer via the access device. In a first access device identification step, ~~wherein~~ the access device communicates to the merchant an identification code associated with the access device. In a second communications establishment step, after the consumer and merchant have agreed on the proposed commercial transaction, the consumer and the electronic identicator use the access device to establish communications with each other. In a second access device identification step, the access device communicates to the electronic identicator the identification code associated with the access device. In a consumer identification step, the electronic identicator compares a bid biometric sample taken directly from the consumer's person with at least one previously registered biometric sample to produce a successful or failed identification of the consumer. In an information forwarding step, upon successful identification of the consumer, the electronic identicator electronically forwards information regarding the consumer to the merchant. Upon successful identification of the consumer, these steps enable a biometrically authorized electronic financial transaction without the consumer being required to present any personalized man-made memory tokens.

Please replace the first full paragraph on page 7, lines 3-7, with the following paragraph:

The access device may be a wireline telephone, a wireless telephone, a two-way pager, a personal digital assistant, or a personal computer. Identification codes associated with an access may include telephone numbers, ~~ESN~~ electronic serial numbers (ESN), a hardware identification code, or encryption of a challenge message using a private key.